8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,072	10/31/2001	Richard L. Schertz	10016864-1	3588

7590 09/19/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
GELAGAY, SHEWAYE	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 09/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/002,072	**Applicant(s)** SCHERTZ ET AL.	
	Examiner Shewaye Gelagay	**Art Unit** 2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on July 21, 2005. Claim 14 has been amended. Claims 1-29 are pending.

Oath/Declaration

2. The objection to the Oath in the first office action is withdrawn.

Claim Rejections - 35 USC § 112

3. The rejection of claim 14 under 35 U.S.C. 112 in the first office action is withdrawn.

Response to Arguments

4. Applicant's arguments filed July 21, 2005 have been fully considered but they are not persuasive. In response to the arguments concerning the previously rejected claims, the following comments are made:

The Applicant argued Rowland (U.S. Patent 6,405,318) does not teach or disclose or even suggest, "an intrusion detection system integrated with an operating system". The Examiner disagrees. Rowland discloses an intrusion detection system that monitors a computer system in real-time by comparing the user behavior to a user profile to detect events that indicate unauthorized entry into the computer. The user profile is dynamically constructed for each computer user and combined with real-time monitoring of log audit files that are login records of a Unix or Windows NT operating system. (Abstract; Col. 4, lines 35-38)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., an operating system having intrusion detection system integrated therein) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The Applicant argues Walsh et al. (hereinafter Walsh, U.S. Patent 5,856,481) does not disclose or suggest, “an anti-virus system integrated into an operating system”. The Examiner disagrees. Walsh discloses an anti-virus system that runs on an operating system in conjunction with a personal computer. Furthermore, Walsh discloses the anti-virus may be implemented in combination with other program modules including routines, programs, components, and data structures. (Abstract; Col. 7, lines 63)

The Examiner disagrees with the applicant and maintains all rejections. All amendments and argument by the Applicant have been considered. It is the Examiner’s conclusion that calms 1-29 are not patentably distinct or non-obvious over the prior art of record in view of the references Rowland, Walsh and Holland. Therefore, all the rejection is maintained as given below.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 22-29 are rejected under 35 U.S.C. 102(b) as being anticipated by Walsh et al. (hereinafter Walsh) United States Letter Patent Number 5,856,481.

As per claim 22:

Walsh teaches a method comprising:

executing an OS-integrated anti-virus system; (Col. 2, lines 63-64) and

monitoring at least one computer resource to detect the presence of at least one virus. (Col. 2, lines 65-67; Col. 3, lines 1-3)

As per claim 23:

Walsh teaches all the subject matter as discussed above. In addition, Walsh further discloses a method wherein monitoring at least one computer resource comprises monitoring at least one computer resource selected from the group consisting of a data storage system, an input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices. (Col. 8, lines 1-6)

As per claim 24:

Walsh teaches all the subject matter as discussed above. In addition, Walsh further discloses a method wherein monitoring at least one computer resource comprises reporting the presence of at least one virus. (Col. 3, lines 1-3 and lines 50-54)

As per claim 25:

Walsh teaches all the subject matter as discussed above. In addition, Walsh further discloses a method wherein the step of monitoring comprises detecting the reassembly of a virus. (Col. 3, lines 50-67; Col. 4, lines 1-5)

As per claim 26:

Walsh teaches all the subject matter as discussed above. In addition, Walsh further discloses a method wherein the step of monitoring comprises recognizing a virus. (Col. 4, lines 28-33)

As per claim 27:

Walsh teaches all the subject matter as discussed above. In addition, Walsh further discloses a method wherein the step of monitoring comprises preventing the storage of a virus. (Col. 3, lines 38-42)

As per claim 28:

Walsh teaches all the subject matter as discussed above. In addition, Walsh further discloses a method wherein the step of monitoring comprises preventing the transmission of a virus. (Col. 10, lines 7-12)

As per claim 29:

Walsh teaches all the subject matter as discussed above. In addition, Walsh further discloses a method wherein the step of monitoring comprises preventing the execution of a virus. (Col. 2, lines 63-67; Col. 3, lines 20-22)

7. Claims 1-3, 15-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Rowland United States Letter Patent Number 6,405,318.

As per claims 1 and 15:

Rowland teaches a computer and a method comprising:

an operating system controlling a computer resource; (Col. 2, lines 40-46) and

an intrusion detection system integrated with the operating system and operable to monitor the computer resources to detect and prevent intrusion attempts. (Col. 2, lines 41-58 and lines 65-67; Col. 3, lines 44-47)

As per claims 2 and 16:

Rowland teaches all the subject matter as discussed above. In addition, Rowland further discloses a computer and a method wherein the computer resource is selected from the group consisting of data storage system, input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices. (Col. 2, lines 263-65; Col. 8, lines 9-23)

As per claims 3 and 17:

Rowland teaches all the subject matter as discussed above. In addition, Rowland further discloses a computer and a method wherein the computer resource comprises an application program execution environment and a networking system under the control of the operating system and monitored by the intrusion detection system to detect, prevent and report intrusion attempts. (Col. 3, lines 44-47; Col. 6, lines 4-6)

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 4-5 and 10-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowland United States Letter Patent Number 6,405,318 in view of Walsh et al. (hereinafter Walsh) United States Letter Patent Number 5,856,481.

As per claims 4 and 5:

Rowland teaches all the subject matter as discussed above. Rowland does not explicitly disclose a computer comprising an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus.

Walsh in analogous art, however, discloses an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. (Col. 2, lines 63-67; Col. 3, lines 1-3; Col. 8, lines 1-6)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Rowland to include an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Walsh (Abstract) in order to have a system that provides protection from infection or damage by a virus and advise the possible danger of spreading the virus.

As per claim 10:

Rowland and Walsh teach all the subject matter as discussed above. In addition, Walsh further discloses an anti-virus system comprises a module operable to prevent reassembly of a virus. (Col. 2, lines 63-67; Col. 3, lines 20-22)

As per claim 11:

Rowland and Walsh teach all the subject matter as discussed above. In addition, Walsh further discloses an anti-virus system comprises a module operable to recognize a virus. (Col. 7, lines 25-41)

As per claim 12:

Rowland and Walsh teach all the subject matter as discussed above. In addition, Walsh further discloses an anti-virus system comprises a module operable to prevent storage of a virus. (Col. 3, lines 38-42)

As per claim 13:

Rowland and Walsh teach all the subject matter as discussed above. In addition, Walsh further discloses an anti-virus system comprises a module operable to prevent transmission of a virus. (Col. 10, lines 7-12)

As per claim 14:

Rowland teaches all the subject matter as discussed above. Rowland does not explicitly disclose a computer wherein the anti-virus system comprises a module operable to prevent execution of a virus.

Walsh in analogous art, however, discloses an anti-virus system comprises a module operable to prevent execution of a virus. (Col. 2, lines 63-67; Col. 3, lines 20-22)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Rowland to include an anti-virus system comprises a module operable to prevent execution of a virus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Walsh (Abstract) in order to have a system that provides protection from infection or damage by a virus.

10. Claims 6-9 and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rowland United States Letter Patent Number 6,405,318 in view of Holland, III et al. (hereinafter Holland) United States Letter Patent Number 6,851,061.

As per claims 6 and 18:

Rowland teaches all the subject matter as discussed above. Rowland does not explicitly disclose a computer and a method wherein intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames.

Holland in analogous art, however, discloses intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. (Col. 2, lines 26-27 and lines 35-36; Col. 5, lines 25-27)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Rowland to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

As per claims 7 and 19:

Rowland teaches all the subject matter as discussed above. Rowland does not explicitly disclose a computer and a method wherein the intrusion detection system is integrated with a networking stack of the networking system above the network layer operable to access reassembled fragments.

Holland in analogous art, however, discloses an intrusion detection system is integrated with a networking stack of the networking system above the network layer operable to access reassembled fragments. (Col. 5, lines 9-22 and lines 29-46)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Rowland to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

As per claims 8 and 20:

Rowland teaches all the subject matter as discussed above. Rowland does not explicitly disclose a computer and a method wherein the intrusion detection system is integrated with a networking protocol stack of the networking system above the transport layer.

Holland in analogous art, however, discloses an intrusion detection system is integrated with a networking protocol stack of the networking system above the transport layer. (Col. 6, lines 29-34; Col. 7, lines 17-42)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Rowland to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

As per claims 9 and 21:

Rowland teaches all the subject matter as discussed above. Rowland does not explicitly disclose a computer and a method wherein the intrusion detection system is integrated with a networking stack of the networking system between the network layer and the transport layer and between the transport layer and the application layer.

Holland in analogous art, however, discloses an intrusion detection system is integrated with a networking stack of the networking system between the network layer and the transport layer and between the transport layer and the application layer. (Col. 6, lines 29-34; Col. 7, lines 17-42)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Rowland to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
09/09/05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100